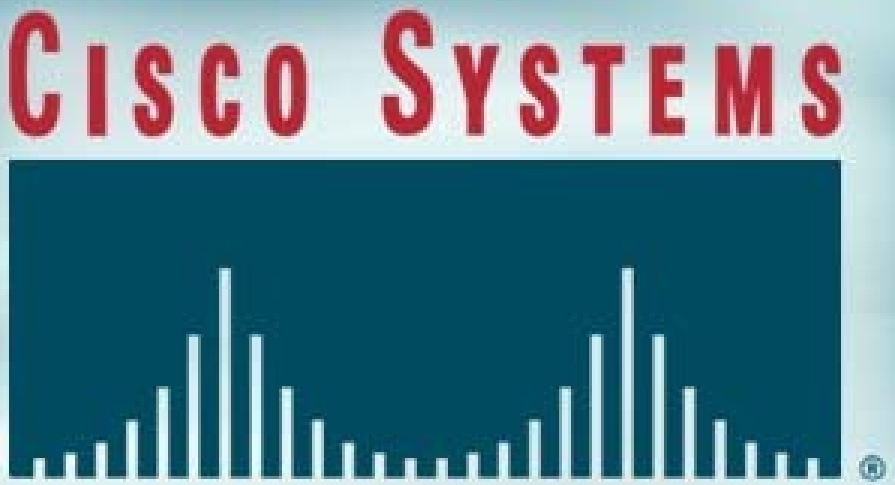
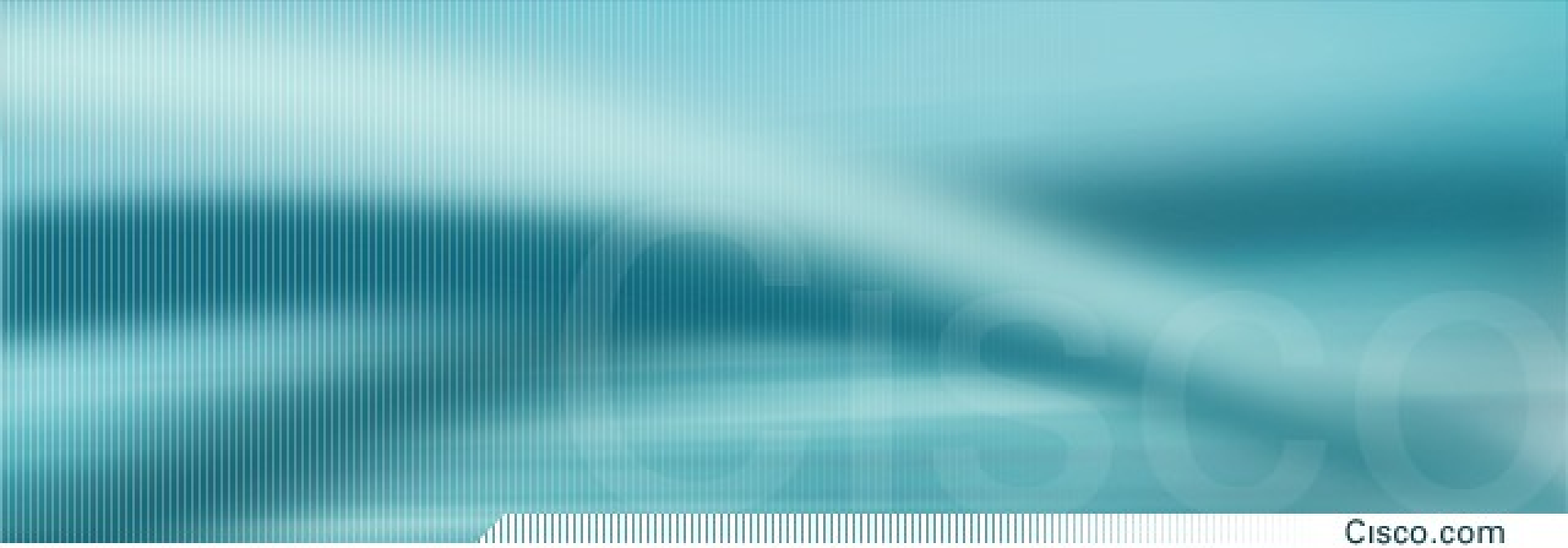

CISCO SYSTEMS



Scalable, Efficient Cryptography for Multiple Security Services

David A. McGrew

Cisco Systems, Inc.

mcgrew@cisco.com

GCM Overview

- **Block cipher mode of operation**
  - **Provides both confidentiality and authentication**
- **Provides high speed, low latency at low cost**
  - **Best mode of operation for packet networks**
- **Usability features**
- **Proposed to NIST and other standards areas**
- **Joint work with John Viega of Secure Software**

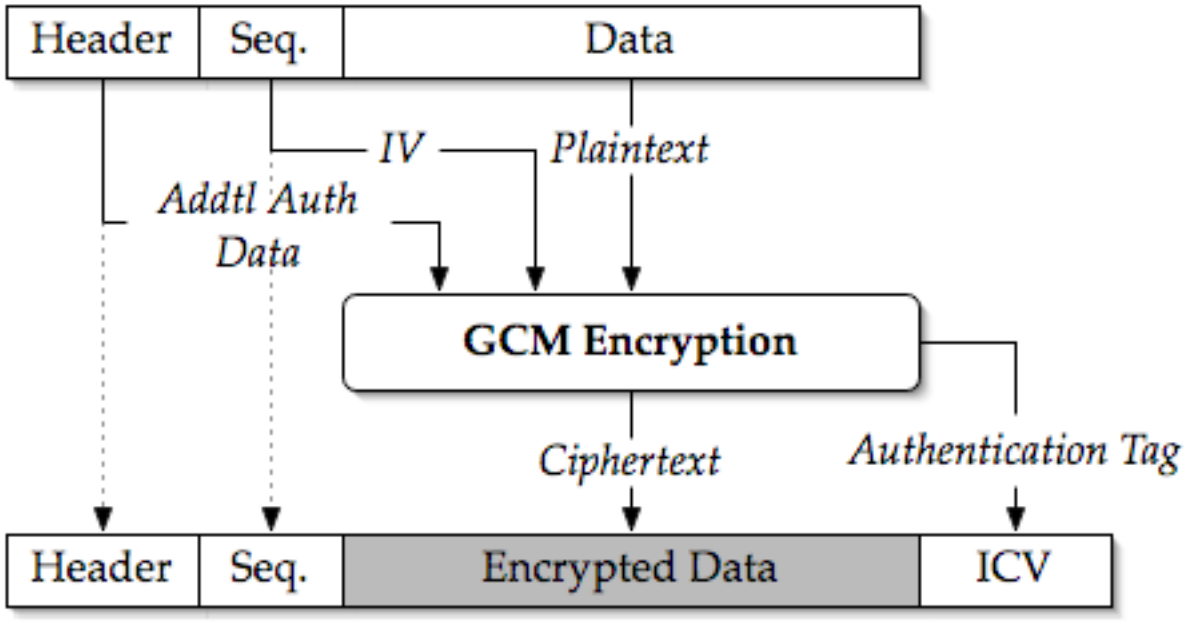
Block Cipher

- **Inputs**
  - ***K* - key**
  - ***P* - plaintext (128 bits)**
- **Output**
  - ***C* - ciphertext (128 bits)**

Authenticated Encryption Operation

- **Inputs**
  - ***K*** **- key (same length as block cipher key)**
  - ***IV*** **- unique value (length between 1 and 2^{64} bits)**
  - ***P*** **- plaintext (length between 0 and 2^{39} bits)**
  - ***A*** **- additional authenticated data (1 to 2^{64} bits)**
- **Outputs**
  - ***C*** **- ciphertext (same length as *P*)**
  - ***T*** **- authentication tag (length between 0 and 128 bits)**

Example: GCM Frame Encryption



AE Mode Requirements

- **Line rate (10+ Gbps) in hardware**
  - **Parallelizable, pipelineable**
  - **Low implementation cost**
  - **Low (packet) latency**
- **Good software performance**
- **Provably secure**
- **Unencumbered by intellectual property**

  Promotes standardization

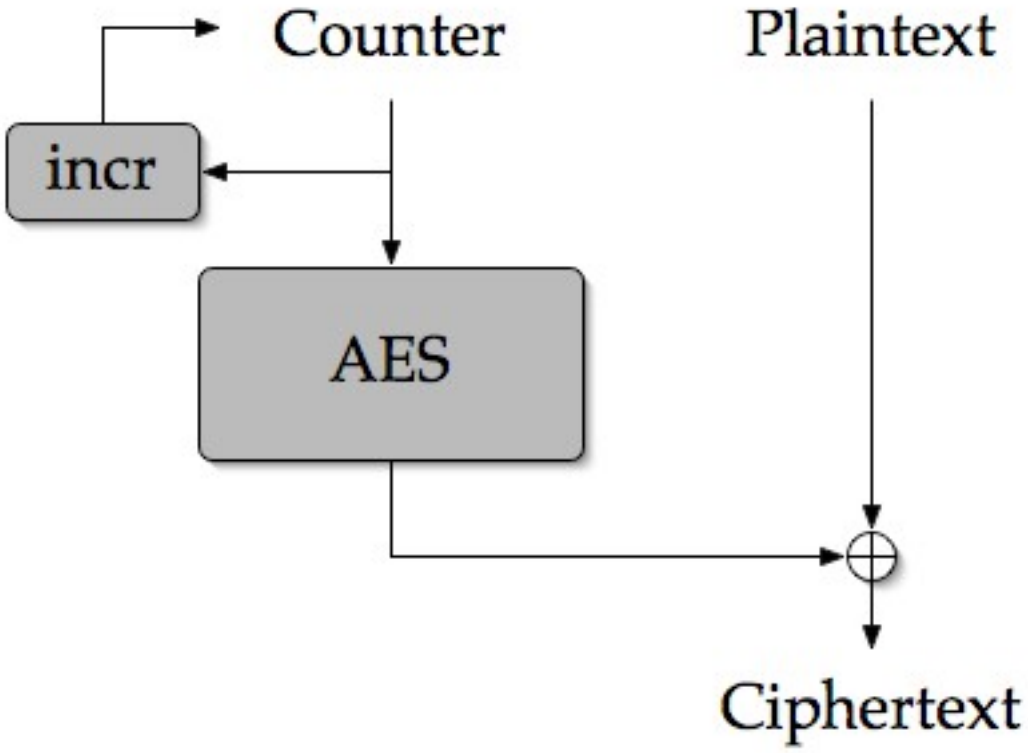
GCM Uses

- **IEEE Link Security (802.1AE)**
  - **GCM is mandatory cryptoalgorithm in draft**
- **IPsec ESP**
  - **Draft based on ESP-AES-CCM, ESP-AES-CTR**
- **Fibre Channel Security**
- **Future fast wireless LAN**

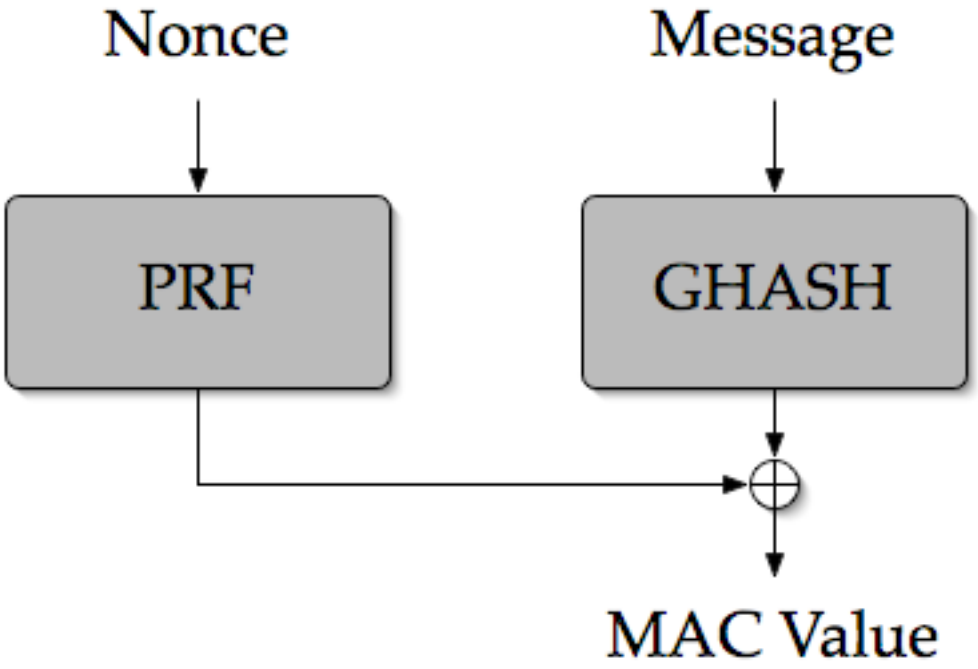
GCM Internals

- **Counter Mode encryption**
  - **Based on IPsec CTR specification**
  - **Efficient, compact**
- **MAC is encrypted hash**
  - **Polynomial hash over GF(2^{128})**
  - **Multiply and accumulate**
- **MAC key $H = E_K(0_{128})$**

Counter Mode Encryption

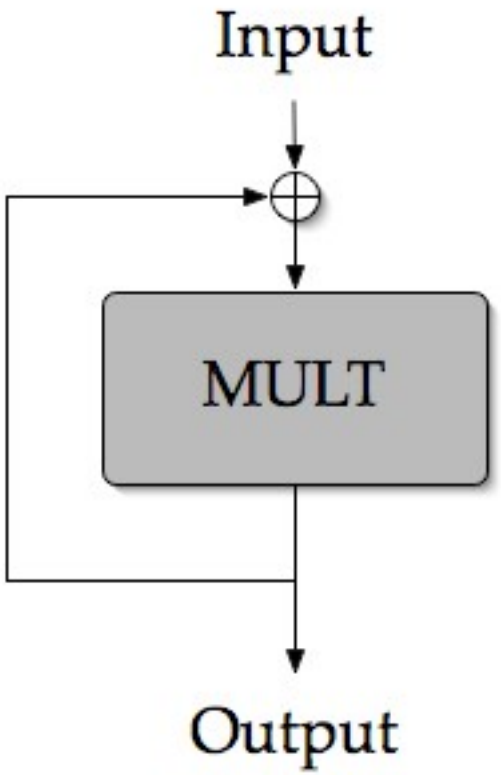


Universal Hash-based MACs



P[GHASH(*M*) ⊕ GHASH(*M'*) = *a*] ≤ ε ~ len(*M*)/2^128

GHASH



Input consists of *C*, *A*, length(A) | length(C)

The Field GF(2^{128})

- **Addition, multiplication, …**
- **Polynomial basis**
  - **Field element ↔ 128 term binary polynomial**
- **Addition is just exclusive-or**
- **Multiplication ~ $128^2 = 2^{16}$ bit operations**
  - **Well-suited for hardware implementations**

Software

- **Counter mode is simple**
  - **Software can avoid first AES round - 10% gain**
- **GF(2^{128}) multiply**
  - **Lookup tables - computed per key**
  - **256 bytes to 64 kilobytes**
- **Fastest mode on packets up to 576 bytes**

Software Performance (cycles/byte)

	CBC + HMAC-SHA1	EAX	CCM	CWC	OCB	GCM256	GCM4K	GCM64K
16	1270	176	89.6	177	89.4	90.5	69.0	58.9
20	995	180	92.0	156	93.3	74.8	57.0	47.8
40	526	111	67.3	111	57.2	54.2	42.0	35.2
44	483	102	62.0	108	53.2	50.0	38.6	31.6
64	342	80.2	58.5	92.8	43.3	45.3	41.6	35.9
128	205	64.2	53.4	79.2	35.6	49.3	37.5	30.4
256	124	56.0	51.1	70.7	31.4	46.8	34.9	30.0
552	83.3	52.9	49.7	65.2	30.6	43.7	33.8	29.3
576	82.5	51.9	49.6	65.5	30.2	43.5	34.3	29.3
1024	68.4	50.6	48.0	63.2	29.3	44.1	33.5	30.1
1500	61.9	49.9	48.6	66.7	29.1	43.8	32.4	30.1
8192	51.2	48.0	47.6	61.2	28.4	44.0	33.3	31.0
Index	**90.3**	**53.4**	**49.6**	**68.3**	**30.8**	**44.0**	**33.3**	**29.9**

Index calculates average cpb assuming:
5% of all traffic is 44-byte packets,
15% of all traffic is in 552-byte packets,
20% of all traffic is in 576-byte packets and
60% of all traffic is in 1,500 byte packets.

GCM Benefits

- **Can act as stand-alone MAC**

  Could be used in IPsec AH or ESP with NULL encryption

- **Can act as *incremental* MAC**
- **Can accept IVs of arbitrary length**

Arbitrary Length IVs

- **Optimized for 96-bit IV**

  Preserves performance, maintains security

- **Promotes usability**

  Can use ‘natural’ nonces – filenames, network addresses, …

  Obviates need to derive secondary keys

Arbitrary Length IV: File Encryption

- ***IV* = seq_num | filename**

  0000 | “/etc/passwd”

  0001 | “/etc/passwd”

  …

- **Authentication tag *T* appended to file**

Incremental MAC

- **Given (MSG, MAC), can compute MAC for MSG ⊕ ∂ efficiently**
- **Useful for remote authentication**
  - **Secure storage networking**
  - **Network filesystems (e.g. CFS)**

Incremental MAC: Remote Storage

- $A = B[0] \mid B[1] \mid \ldots \mid B[N\text{-}1]$
- $P = \{\}$
- IV = version number (plus other info)
- When $B[i]$ is changed to $B'[i]$, compute

  New T = Old T ⊕ AES(Old IV) ⊕ AES(New IV) ⊕ HASH(H, $B[i]$) ⊕ HASH(H, $B'[i]$)

Security

- **Counter mode well understood**
  - **AES GCM secure up to ~ 2^68 bytes**
- **MAC based on XOR-universal hash**
  - **Well understood theory**
  - **Good security properties**

Security Considerations

- **IV reuse in encryption can expose *H***
  - **But reuse in decryption does not**
- **Given one forged message, can produce many more easily**
  - **But does not change likelihood of zero forgeries**
- **All-zero counter value is highly unlikely and undetectable**

References (1 of 2)

- **GCM and OCB**
  - csrc.nist.gov/CryptoToolkit/modes/proposedmodes/
- **IEEE Link Security**
  - www.ieee802.org/1/pages/802.1ae.html
  - www.ieee802.org/linksec/
- **Fibre Channel**
  - www.t11.org/
  - www.fibrechannel.org/
- **IPsec**
  - draft-ietf-ipsec-ciph-aes-gcm-00.txt

References (2 of 2)

- **Counter mode**

  Diffie and Hellman. Privacy and Authentication: An Introduction to Cryptography. *Proceedings of the IEEE*, Volume 67, Number 3, March, 1979.

  Bellare, Desai, Jokkipi, and Rogaway. A concrete security treatment of symmetric encryption, *Proceedings of 38th Annual Symposium on Foundations of Computer Science*, IEEE, 1997.

- **Universal hashing and MACs**

  Wegman and Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*. Vol. 22, 265-279, 1981.

  Krawczyk. LFSR-based hashing and authentication. Proceedings of CRYPTO '94. *Lecture Notes in Computer Science No. 839*, 129-139.

Comparison to OCB

- **GCM has slightly higher per-block cost**
  - **GF(2^{128}) multiply**
- **OCB has extra per-packet AES invocation**
  - **Adds AES latency to packet encryption latency**
- **Software: GCM faster on short packets**
- **Hardware: GCM slightly higher cost, 1/2 latency**
- **GCM may need additional key store**
- **GCM has additional benefits**

Security Model (1 of 2)

- **Block cipher is secure if indistinguishable from a random permutation**
- **GCM secure if**
  - **Ciphertext indistinguishable from random, and**
  - **Forgery unlikely to succeed**

Security Model (2 of 2)